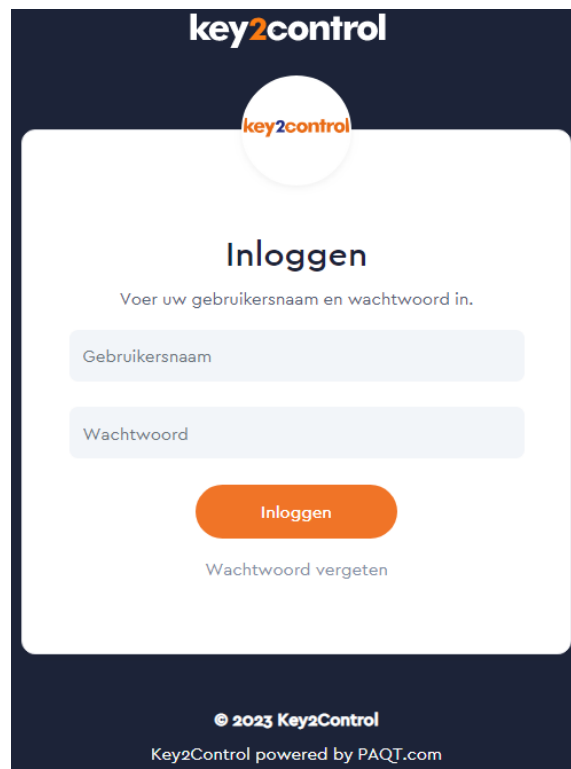


Haal meer rendement uit de software van Key2Control "De basismodule"



The image shows a login interface for Key2Control. At the top, the 'key2control' logo is displayed in white on a dark blue background. Below the logo is a circular icon containing the 'key2control' text. The main heading is 'Inloggen' (Login). Below this, a subtitle reads 'Voer uw gebruikersnaam en wachtwoord in.' (Enter your username and password). There are two input fields: 'Gebruikersnaam' (Username) and 'Wachtwoord' (Password). Below the password field is an orange 'Inloggen' button. A link for 'Wachtwoord vergeten' (Forgot password) is located below the button. At the bottom, the footer contains '© 2023 Key2Control' and 'Key2Control powered by PAQT.com'.

Dit document is bedoeld voor klanten van Key2Control die al bekend zijn met de basisfunctionaliteit van onze software. Het document bevat handige tips die bijdragen tot meer rendement en gebruiksgemak van onze software.

Key2Control
Datum: mei 2023
Versie 1.1

Inhoudsopgave

1	INLEIDING.....	3
2	DE NULMETING.....	5
2.1	UITVOEREN METING 1	5
2.2	AFRONDEN METING 1.....	6
2.3	PRIORITEREN	7
2.4	PLANNEN ACTS.....	8
3	DE INZET EN MEERWAARDE VAN CHECKS	10
3.1	VERSCHIL TUSSEN METEN EN CHECKS	10
3.2	PLANNEN EN MONITOREN VAN CHECKS.....	11
3.3	CHECKS ALS INPUT VOOR METING.....	12
4	OBJECTENMODULE	13
4.1	OBJECTEN KOPPELEN AAN MAATREGELEN	14
4.2	OBJECTEN ALS CENTRAAL VERZAMELPUNT	15
4.3	PRAKTIJKVOORBEELD GEBRUIK OBJECTEN / INFORMATIEBEVEILIGING.....	16
5	BEHEERSINGSMODEL EN REPETERENDE BEHEERACTIVITEITEN	18
5.1	ALGEMEEN	18
5.2	INTERN BEHEERSINGSMODEL IN RELATIE TOT KEY2CONTROL SOFTWARE.....	18
5.3	GANGBARE BEHEERSINGSPRINCIPES IN RELATIE TOT KEY2CONTROL SOFTWARE.....	20
5.4	PERIODIEKE RAPPORTAGES	21
5.5	OPSTELLEN PLANNINGSSCHEMA.....	23
5.6	BESCHIKBARE RAPPORTAGES IN KEY2CONTROL	24
6	TOT SLOT	26

1 Inleiding

Het gebruik van onze software ondersteunt het interne beheersingsproces van onze klanten en helpt hen bij het realiseren van hun ambities op dit gebied. De vele reacties die we ontvangen uit klantbetrokkenheidsonderzoeken over het gebruik van onze software zijn uitermate positief, en dat inspireert ons om onze kennis en ervaring met u te delen. We leren namelijk ook van het gebruik en de doorontwikkeling van onze software en zien mogelijkheden om het rendement van het gebruik ervan te vergroten. Deze kennis komt voort uit de praktijk. Dit jaar hebben we dit inputkanaal verder geprofessionaliseerd door middel van expertgroepen.

Dit document is een update van versie 1.0 uit 2022 en aangevuld met nieuwe functionaliteit in de software en voortschrijdende inzichten in het gebruik ervan. Zo is ook de objectenmodule in dit document opgenomen in relatie tot het gebruik van normenkaders. Voor de herkenbaarheid proberen we zoveel mogelijk dezelfde opbouw te hanteren als in de vorige versie. Dit document is echter geen cursus waarin de basisfunctionaliteit van de software wordt uitgelegd, maar bevat talloze tips om het gebruik van onze software beter toe te passen in de praktijk, gericht op continue verbetering. Naast tips over het gebruik van onze software gaan we ook impliciet in op de volgende vragen:

- 1) Hoe kan de software bijdragen aan een stabiele beheerorganisatie?
- 2) Hoe zorgen we ervoor dat het management betrokken blijft bij het interne beheersingsproces?
- 3) Hoe kan het gebruik van de software worden vergroot, zodat de beheerorganisatie minder kwetsbaar is bij uitval van een of meerdere sleutelfunctionarissen?

Een stabiele beheerorganisatie is de opmaat om beheersdoelstellingen op een betrouwbare wijze te realiseren (governance), onzekerheden aan te pakken (risicobeheer) en integer te handelen (compliance). En dat is precies waar interne beheersing om gaat. De laatste vraag wordt steeds relevanter vanwege een toenemende in- en uitstroom van personeel bij onze klanten, waardoor kennisverlies kan optreden en het beheersingsproces telkens opnieuw moet worden uitgevonden. Het borgen van kennisbehoud krijgt dan ook steeds meer aandacht. Dat kennisbehoud is een van de sterke punten van onze software.

Kenmerken van een stabiele beheerorganisatie zijn onder meer:

- a) Het toepassen van het drielijnenmodel (governance) waarin taken en verantwoordelijkheden in de beheerorganisatie zijn vastgesteld en geïmplementeerd. Dan gaat het om het proces rondom de PDCA-cyclus.
- b) Het toepassen van een gestandaardiseerde aanpak die bijdraagt in consistentie in de manier waarop interne beheersing wordt geïmplementeerd en gecontroleerd,

waardoor inconsistenties en fouten worden verminderd. Dit vergroot eveneens de betrouwbaarheid van interne beheersing.

- c) Samenwerking omdat het de uitwisseling van 'best practices' bevordert, wat het lerend vermogen van de organisatie ten goede komt. Het verhoogt het bewustzijn van alle belanghebbenden en draagt bij aan de adoptie en borging van het interne beheersingsproces.
- d) Samenhang van de verschillende aspecten van interne beheersing voor het behalen van een optimaal resultaat van bedrijfs- en beheersdoelstellingen. Het gaat dan vooral om het in balans brengen van deze beheersingsprincipes. Door bijvoorbeeld te veel te leunen op risicobeheer kan een onbalans ontstaan met onnodig veel overhead en een verstikkend effect op de bedrijfscultuur.

Het gebruik van onze software ondersteunt alle beheersingsprincipes en daarmee de weg naar een stabiele beheerorganisatie.

In dit document behandelen we de basismodule ofwel het deel waarin de PDCA-cyclus is opgenomen voorzien van voorgedefinieerde toetsbare normenkaders. Daarbij betrekken we ook de objectenmodule. De risico- en auditmodule worden (vooralsnog) niet behandeld in dit document, hoewel er in enkele gevallen wel naar beide modules wordt verwezen. Het document volgt de uitvoering van een meting ook wel zelfevaluatie van een normenkader en de daaruit voortvloeiende handelingen volgens de PDCA-cyclus.

We hebben een tweetal handige tips uit dit document geselecteerd die zeker zullen bijdragen tot een beter gebruik van de software.

1. Maak na afronding van meting 1 direct een nieuwe meting aan (meting 2) door een kopie te maken van meting 1 en houd deze meting gedurende het hele jaar open in plaats van deze af te ronden. Deze aanpak biedt diverse voordelen die vermeld staan in paragraaf 2.1.
2. Gebruik 2 tabbladen in de webbrowser bij het afstemmen van acts en checks met een openstaande meting. In de eerste tabblad houd je de meting open, terwijl je in de andere tabblad het takenmanagement van het betreffende normenkader opent en op deze wijze snel kan switchen en kopiëren.

Door de URL van Key2Control te kopiëren naar een tweede tabblad in de webbrowser wordt de software nogmaals opgestart. Zo kan je verschillende normenkaders met elkaar vergelijken of verschillende metingen van hetzelfde normenkader openen en vergelijken. Het gebruik van meerdere tabbladen biedt flexibiliteit en efficiëntie bij het werken met de software.

2 De nulmeting

2.1 Uitvoeren meting 1

Elk nieuw voorgedefinieerd normenkader dat geactiveerd wordt, begint met een nulmeting bedoeld om inzicht te krijgen waar de organisatie staat ten aanzien van dat normenkader. Een normenkader bevat een samenhangende set van toetsbare normen die tijdens een meting voorzien moet worden van een kwalificatie. Dat kan zijn 'niet van toepassing', 'ja', 'deels' of 'niet' geïmplementeerd. Ter ondersteuning hiervan bevat elke norm een toelichting op de norm en 'gesloten' stuurvragen die elk beantwoord kunnen worden. Dit geheel helpt om antwoord te geven in hoeverre de norm is geïmplementeerd. Het is overigens niet verplicht de stuurvragen te beantwoorden, maar het helpt wel.

Het eindresultaat van een meting is een grafisch overzicht voorzien van een gemiddelde score per hoofdstuk en in totaal. De neiging is aanwezig om bij de eerste meting direct diep in te zoomen op alle gestelde stuurvragen en dat vergt relatief veel tijd.

Verstandiger is om in de beginfase 'luchtiger' door de vragen heen te gaan en dit verder aan te scherpen bij de volgende meting(en). Daarmee bespaar je tijd en heb je wel een beeld op hoofdlijnen waar de organisatie staat. Je stapt immers in een jaarlijkse PDCA-cyclus die gericht is op continu verbeteren voor het betreffende normenkader.

De nulmeting heeft voornamelijk tot doel een eerste beeld te krijgen van de positie van de organisatie met betrekking tot het normenkader. Dit beeld hoeft niet meteen volledig accuraat te zijn. Een korrelige vakantiefoto (polaroid foto) van het strand waarbij er duidelijk onderscheid is tussen de zee en het landschap is voldoende. Waar het om draait, is dat deze foto intern besproken kan worden met de verantwoordelijke personen om te bepalen of we ons hierin kunnen vinden. Herkenning is een eerste stap naar structurele verbetering en bewustwording van hun rol op het gebied van interne beheersing. De interactie en verbinding tussen de 1e en 2e lijn is immers cruciaal voor verdere groei op de volwassenheidsladder.

Tips bij een nulmeting:

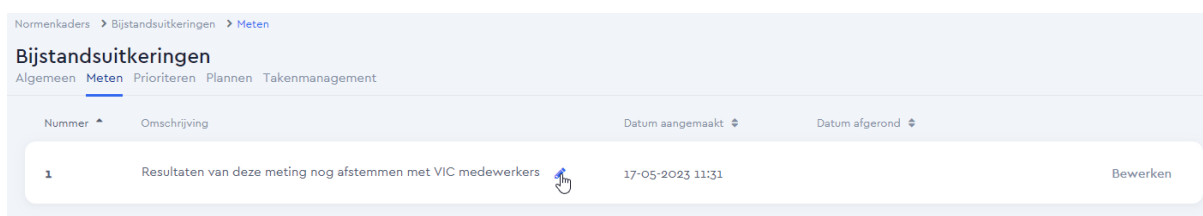
- 1) Als er geen duidelijk antwoord gegeven kan worden op een norm, geef dit dan aan in het commentaarveld en kwalificeer het als "deels" of "nee" (immers bij twijfel niet inhalen!). Dit punt kan vervolgens verder worden onderzocht via prioritering. Deze werkwijze bespaart veel tijd!
- 2) Vul voor elke norm het commentaarveld in met de informatie die op dat moment bekend is, zelfs als je voldoet aan de norm. Hiermee leg je kennis vast die later kan worden hergebruikt bij een volgende meting.
- 3) Sla eventueel stuurvragen over waarop je geen antwoord kunt geven. Geef indien nodig de reden hiervoor aan in het commentaarveld.

- 4) Vermeld bij elk commentaar een datum. Dit kan later (bijvoorbeeld bij een volgende meting) dienen als een soort logboek. Zo kun je zien hoe het commentaar bij elke norm zich in de loop der tijd ontwikkelt.

Nadat alle normen zijn gekwalificeerd en voorzien zijn van commentaar, kan er een eerste grafisch overzicht worden weergegeven. Deze voorlopige resultaten kunnen intern worden besproken en indien nodig worden aangepast in de software. Het is immers belangrijk om te benadrukken dat de meting nog niet is afgerond. Op deze manier is er ruimte voor wijzigingen tijdens de afstemming met andere belanghebbenden. Binnen het onderdeel 'Meten' zijn drie rapportages beschikbaar waaronder een verklaring van toepasselijkheid. In paragraaf 5.4 gaan we nader in op deze rapportages.

Tips:

- 5) Rond de meting in deze fase nog niet af. Het afronden van de meting maakt deze immers definitief en het is dan niet meer mogelijk om aanpassingen aan te brengen.
- 6) Exporteer het rapport meting normenkaders (Excel) bij het onderdeel 'Meten' en controleer of alle commentaarvelden correct zijn ingevuld. Uiteraard kan ook gebruik worden gemaakt van het rapport 'Meting en gap-analyse', waarin tevens de stuurvragen zijn opgenomen, maar dit is een omvangrijk document en vooral bedoeld voor eigen gebruik.
- 7) Maak gebruik van het tekstveld 'Omschrijving', dat beschikbaar is voor elk meetnummer. Zie hieronder een voorbeeld van een printscreen voor meetnummer 1.



The screenshot shows a web application interface for 'Bijstandsuitkeringen'. It has a breadcrumb trail: 'Normenkaders > Bijstandsuitkeringen > Meten'. Below the title, there are tabs: 'Algemeen', 'Meten' (selected), 'Prioriteren', 'Plannen', and 'Takenmanagement'. A table displays measurement data with columns: 'Nummer', 'Omschrijving', 'Datum aangemaakt', and 'Datum afgerond'. The first row shows '1' for the number, 'Resultaten van deze meting nog afstemmen met VIC medewerkers' for the description, and '17-05-2023 11:31' for the creation date. There is a 'Bewerken' (Edit) button at the end of the row.

Nummer	Omschrijving	Datum aangemaakt	Datum afgerond
1	Resultaten van deze meting nog afstemmen met VIC medewerkers	17-05-2023 11:31	

Op deze manier kunnen aantekeningen op meetniveau worden vastgelegd onder 'Omschrijving'. Denk bijvoorbeeld aan het registreren van de wijze van afhandeling van de betreffende meting of aan opvallende zaken die voortkomen uit de meting die je wilt bespreken. Dit tekstveld kan op elk moment worden aangepast, ongeacht of de meting is afgerond of niet.

2.2 Afronden meting 1

Als duidelijk is dat er geen verdere aanpassingen meer nodig zijn, maken we de meting definitief door op de knop 'Afronden' te drukken. De afrondingsdatum wordt automatisch vermeld bij de desbetreffende meting. Na bevestiging word je automatisch naar het

tabblad 'Prioritering' gebracht. Daar zijn alle acts weergegeven die gekoppeld zijn aan een norm die deels of niet geïmplementeerd zijn. Meting 1 is dan definitief.

Tip:

- 1) Maak na afronding van meting 1 direct een nieuwe meting aan (meting 2) door een kopie te maken van meting 1 en houd deze meting het hele jaar open (dus niet afronden).
- 2) Het is overigens mogelijk om alle opgeslagen documenten uit de oude meting mee te kopiëren naar de nieuwe meting. Denk aan documenten die een relatief vast en langdurig karakter hebben.

Het direct aanmaken van een nieuwe meting na afronding biedt diverse voordelen:

- a) Het biedt de reporter de mogelijkheid om tussentijds de kwalificatie van normen, stuurvragen en commentaar (met vermelding van datum) aan te passen. De input hiervoor kan komen uit nieuwe inzichten, gevoerde gesprekken, externe rapporten en resultaten uit acts en checks.
- b) Tussentijds heb je altijd een actueel overzicht en een actuele score die kan afwijken van de score uit meting 1. Zo is het mogelijk een verschillenanalyse uit te voeren, bijvoorbeeld ten behoeve van een voortgangsrapport.
- c) Doordat de meting actueel blijft, kan aan het begin van de nieuwe jaarcyclus (bijvoorbeeld in januari) deze meting snel worden afgerond en direct meting 3 worden opgestart door een kopie te maken van meting 2.

Meting 2, die het hele jaar openstaat, heeft geen invloed op de prioritering en planning die gebaseerd zijn op meting 1, die de status "afgerond" heeft. Op het moment dat meting 2 wordt afgerond, schakelt de software automatisch over naar de prioritering op basis van de resultaten uit meting 2. Het resultaat van meting 2 zal in principe scherper zijn dan dat van meting 1 vanwege de betere inzichten die tussen meting 1 en 2 zijn ontstaan en de doorgevoerde verbeteringen. Dit is het gevolg van het consequent volgen van de PDCA-cyclus die gericht is op continu verbeteren.

2.3 Prioriteren

In de voorgesprekken over de resultaten van de meting met leidinggevenden of direct betrokkenen is het verstandig om aan te geven welke verbeteringen de komende periode doorgevoerd moeten worden en welke voorlopig overgeslagen worden. Op die manier betrek je de verantwoordelijken bij het beheersingsproces. Vertaald naar de software komt dit neer op het geven van een hoge of lage prioritering. Een hoge prioritering betekent dat je van plan bent om deze act in deze periode te plannen voor verbetering. Een lage prioritering betekent dat deze act overgeslagen wordt, ook al is de bijbehorende norm deels of niet geïmplementeerd. Het uitgangspunt is dat ALLE acts een hoge of lage prioritering hebben. Hoe bepaal je nu de prioritering?

Dat is een afwegingsproces, bijvoorbeeld door je eerst te richten op 'laaghangend fruit'. Maar het is ook een kwestie van het afwegen van risico's. Het belangrijkste is dat je dit afwegingsproces gezamenlijk doorloopt. Het is helemaal niet erg om bepaalde acts een lage prioriteit te geven. Deze blijven namelijk wel in beeld en wellicht worden ze in de volgende cyclus opgepakt. Bij het prioriteren is het ook belangrijk om je af te vragen of het aantal acts met een hoge prioriteit daadwerkelijk gerealiseerd kan worden in het betreffende beheersjaar. Stem dat bijvoorbeeld af op de beschikbare menscapaciteit. Zorg in ieder geval voor een realistische planning. Het is namelijk vervelend om een planning formeel vast te stellen, terwijl op voorhand al bekend is dat deze niet realistisch is. Dan krijg je aan het einde van het jaar kritiek en moet je uitleggen waarom de planning niet is gerealiseerd.

2.4 Plannen acts

In de tab planning staan bovenaan de hoog geprioriteerde acts met de volgende kenmerken:

Kenmerk: **Act** **Hoge prioriteit** **Uit meting** **Niet ingepland**

De blauwe stempel (uit meting) geeft aan dat het een verbeterpunt is dat voortkomt uit de laatst afgeronde meting (in dit voorbeeld dus meting 1). De oranje stempel (hoge prioriteit) geeft aan dat deze act gepland moet worden en voortkomt uit de prioritering.

Door op de betreffende act te klikken opent de software het planningsgedeelte. Daar worden de naam van de uitvoerder en de reviewer vermeld evenals de geplande opleverdatum, het beheersjaar en de werkinstructie. Elke geplande act behoort een werkinstructie te hebben, anders weet de uitvoerder niet wat er van hem/haar verwacht wordt.

Tips:

- 1) Zorg ervoor dat de werkinstructie zodanig beschreven is dat de uitvoerder deze begrijpt. Geef aan wat er moet gebeuren en wat opgeleverd moet worden. Als er bewijs opgeleverd moet worden, geef dit dan ook als zodanig aan. Kortom, maak de werkinstructie zo concreet mogelijk. Dat is ook van belang voor de reviewer. De input voor werkinstructies komt in dit geval uit meting 1.
- 2) Stem zo nodig deze werkinstructies vooraf af met de betrokken uitvoerders, bijvoorbeeld in een workshop. Vraag hen persoonlijk of ze begrijpen wat de bedoeling is.
- 3) Als de verbetering omvangrijk en langdurig is, dus langer dan een jaar, knip het geheel dan in behapbare stukjes die via acts volgtijdelijk worden aangeboden en gedoseerd. Plan alleen datgene wat in het lopende beheersjaar opgeleverd moet worden.

- 4) Als nog niet duidelijk is wie de uitvoerder is, plan de act dan in eerste termijn op je eigen naam en pas de naam van de uitvoerder aan zodra de naam bekend is van degene die daadwerkelijk belast wordt met de betreffende taak en bekend is met de instructies voor het uitvoeren van een taak in Key2Control.

Niet-planmatig onderhoud

Een act is overigens een eenmalige actie en wordt in dit geval geïnitieerd vanuit een meting. Wij noemen dit 'planmatig onderhoud' dat voortkomt uit een PDCA-cyclus. De realiteit is echter weerbarstiger. Soms is er plotseling een verbetering nodig die niet voortkomt uit een meting, maar bijvoorbeeld naar voren komt uit een audit- of adviesrapport of tijdens een gesprek met een van je collega's. In dat geval is het ook mogelijk om dergelijke niet-planmatige verbeteringen te plannen. We gaan dan direct naar de planning, slaan dus de prioritering over (aangezien deze gericht is op 'planmatig onderhoud' op basis van een meting) en volgen de volgende stappen:

- a) Vanuit het filter 'selecteren' schakelen we alle vinkjes uit behalve die van de acts. Op deze manier hebben we alle acts in beeld en is de invloed van de meting op de planning (tijdelijk) tenietgedaan.
- b) Daarna selecteren we de desbetreffende act (door te zoeken op normnummer of te scrollen) en plannen we de act zoals eerder beschreven.

Tips:

- 4) Vermeld bij de werkinstructie van een niet-planmatige act de trigger waar deze actie vandaan komt.
- 5) Werk je openstaande meting bij voor de betreffende norm of normen op dit punt. Dit kan reden zijn om de kwalificatie (wel, deels of niet geïmplementeerd) bij de betreffende norm aan te passen.

Het kan ook voorkomen dat het om een niet-planmatige verbetering gaat waarvoor geen act beschikbaar is onder een van de normenkaders. In dat geval kan gebruik gemaakt worden van de risicomodule. De voorgestelde verbetering wordt dan als een risico gedefinieerd. Via takenmanagement in de risicomodule kan deze act op dezelfde wijze worden beheerd als onder de normenkaders.

Tips:

- 6) Indien de risicomodule niet beschikbaar is, selecteer dan een act uit het normenkader die de verbetering het dichtst raakt en vermeld in de werkinstructie waar het over gaat en wat verbeterd en opgeleverd moet worden.
- 7) Een andere optie is om een apart object te definiëren dat specifiek wordt gebruikt voor dit doel. Koppel dit object aan een act, zodat duidelijk is dat het om een verbetering gaat die geen verband houdt met de betreffende norm. Zie voor verdere toelichting paragraaf 4.1.

3 De inzet en meerwaarde van checks

3.1 Verschil tussen meten en checks

Checks zijn feitelijk tussentijds geplande metingen van een norm die door een uitvoerder worden afgehandeld. De checks worden toegewezen aan degenen die verantwoordelijk zijn voor het naleven van de gestelde eisen. Dit kunnen verschillende personen zijn die allemaal input leveren aan het normenkader. Meestal zijn dit personen in de 1e lijn. Het gebruik van checks heeft twee doelen: ten eerste om zoveel mogelijk verantwoordelijkheid neer te leggen bij degenen die belast zijn met de betreffende beheeractiviteiten die in de checks worden behandeld. Door deze checks jaarlijks herhaaldelijk te plannen, raken zij vertrouwd met de gestelde eisen, wat bijdraagt aan kwaliteitsverbetering en een hoger bewustzijn van hun bijdrage aan het normenkader. Een bijkomend voordeel is dat dit de reporter ontlast, zodat hij zich meer kan richten op zijn rol van monitoring in het beheersingsproces.

Het tweede doel van checks is om tussen twee metingen door een actueel beeld te behouden, vooral voor die checks die gerelateerd zijn aan risicovolle normen (zie verder). Voor de reporter leveren checks belangrijke input uit de eerste hand op. Een check kan in de beeldspraak van een thermometer worden beschouwd om tussentijds de temperatuur te meten. In die zin zou de afhandeling van een check gemiddeld 3 minuten in beslag nemen. Als het langer duurt, is dat een indicatie dat de uitvoerder nog niet vertrouwd is met de gestelde eisen. Een check is dus niet bedoeld om zaken uit te zoeken, maar om aan te geven hoe het ervoor staat.

Wat is nu het verschil tussen meten en checks? Meten is primair bedoeld voor planmatig onderhoud volgens de PDCA-cyclus en vindt plaats onder beheer van de reporter, om zo de jaarlijkse verbeteringen (acts) in kaart te brengen. Het is een momentopname om alle relevante informatie te verzamelen voor het identificeren van verbeterpunten (acts). Meestal gebeurt dit jaarlijks aan het begin van het nieuwe jaar. Het uitvoeren van checks daarentegen is een doorlopend proces om tussentijds zoveel mogelijk actuele informatie te verzamelen over de status van de normen en is niet gebonden aan de resultaten van een meting.

Door consequent jaarlijks te meten volgens de PDCA-cyclus ontwikkelt de reporter een tijdlijn over de ontwikkeling van het normenkader weergeeft. Er wordt als het ware een fotoboek gecreëerd waarop kan worden teruggekeken en de basis vormt voor het op een controleerbare wijze afleggen van verantwoording.

Overigens is het niet nodig om elke check te plannen, maar wel de checks die gerelateerd zijn aan risicovolle normen (keycontrols) of waarvan jaarlijks bewijslast vereist is. Deze afweging wordt gemaakt op basis van een risico-inschatting. Het kan

bijvoorbeeld zo zijn dat de ene check maandelijks gepland wordt, de andere per kwartaal en weer een andere jaarlijks. De risicomodule van Key2Control kan hierbij van nut zijn. Hoe meer risico's met een hoog risicoprofiel gekoppeld zijn aan een norm, des te groter het belang van die norm.

Tips:

- 1) Bepaal vooraf welke checks periodiek gepland moeten worden.
- 2) Plan alleen in het betreffende beheersjaar en plan niet jaren vooruit.
- 3) Bepaal wie de uitvoerder en reviewer zijn voor elke check.
- 4) Bespreek vooraf met de uitvoerders wat de bedoeling is en of zij bereid zijn deze taken uit te voeren.
- 5) Indien de checks van een normenkader goed gepland zijn voor jaar 1, kunnen deze checks eenvoudig gepland worden voor jaar 2 met dezelfde frequentie en dezelfde werkinstructie via takenmanagement door te klikken op 'Toevoegen' bij de betreffende taak.

De bekende argumenten 'geen tijd' en 'ik heb het al zo druk' zijn hier niet van toepassing. Zoals eerder vermeld, vergt de afhandeling van een check gemiddeld 3 minuten. Sterker nog, het gepland uitvoeren van taken levert tijd op voor de uitvoerder. Bij interne controle of audits kan de betreffende uitvoerder verwijzen naar reeds afgehandelde taken in Key2Control. Bovendien biedt deze vastlegging ook een referentiekader voor de uitvoerder zelf (hoe heb ik dit ook alweer gedaan?) en voor zijn toekomstige opvolger (hoe heeft mijn voorganger het gedaan).

Gebruikers moeten zich realiseren dat ze deel uitmaken van een groter geheel dat gericht is op het verbeteren van de kwaliteitsuitvoering en het op een controleerbare wijze afleggen van verantwoording. Je kunt het vergelijken met een analoge horloge waarin alle radartjes moeten samenwerken om de juiste tijd aan te geven. Er zijn altijd andere belanghebbenden die op een ander niveau gebruik moeten maken van de input die wordt geleverd door de uitvoerders. Op die manier creëer je een basis voor optimalisatie (samen met iedereen) in plaats van suboptimalisatie (voor mij alleen).

3.2 Plannen en monitoren van checks

Vanuit een oogpunt van gewenning is het advies om het plannen van checks gefaseerd te laten verlopen. Dit kan bijvoorbeeld door de checks eerst op naam van de reporter te plannen en zodra de uitvoerders bekend zijn, de taken aan de juiste uitvoerders toe te wijzen.

Op deze manier werk je onbewust aan het verfijnen van de governance op de werkvloer wat bijdraagt aan een stabiele beheerorganisatie. Nadat de juiste uitvoerders zijn toegewezen aan de checktaken, is het belangrijk dat zij deze taken tijdig uitvoeren. Hier

speelt de reporter een belangrijke monitoringrol. Als sprake is van achterstand in de planning, is het de taak van de reporter hen hierop te wijzen. Dit kan bijvoorbeeld door direct het gesprek aan te gaan in combinatie met een voortgangsrapport volgens de PDCA-cyclus.

Het plannen van checks verloopt op dezelfde manier als bij acts, met als verschil dat checks niet eenmalig zijn, maar voortdurend worden gepland ongeacht de uitkomst. In de werkinstructie van een check hoef je niet aan te geven wat de bedoeling is. De check zelf bevat een duidelijke toelichting en stuurvragen die beantwoord moeten worden.

Tips:

- 1) Plan checks alleen in het lopende beheersjaar en niet in toekomstige beheersjaren.
- 2) Geef in de werkinstructie van een check aan welke bewijslast opgeleverd moet worden. Maak dit zo concreet mogelijk. Dit kan één of meerdere documenten, een printscreen, een link of een verwijzing zijn.
- 3) Zorg ervoor dat de uitvoerder de stuurvragen en het commentaarveld invult en de taak voorziet van bewijslast.
- 4) Attendeer de reviewer hierop. Als de uitvoerder het commentaarveld niet heeft ingevuld of geen bewijslast heeft geleverd, keur de taak dan af als reviewer en geef informatie waarom de taak is afgekeurd.
- 5) Als de uitvoerder het niet weet of begrijpt, geef dit dan aan in het commentaarveld met als score 'onvoldoende'. Dit is bruikbare informatie voor de reporter om bij te kunnen sturen.

In het begin kan bij sommige uitvoerders frictie ontstaan door de gestandaardiseerde werkwijze. Het is immers een proces dat tijd vergt om aan te wennen en dit moet goed worden opgevangen. Daar ligt een belangrijke taak voor de reporter. De software biedt hiervoor de benodigde stuurinformatie zoals achterstand in de planning, om tijdig actie te ondernemen. Een belangrijk voordeel voor de reporter is dat hij overzicht heeft van de openstaande taken en zich alleen hoeft te richten op de uitvoerders die achterstand hebben. Naarmate uitvoerders vertrouwd raken met hun periodieke checktaken, zal de omvang van de achterstand beperkter worden. Dat is waar we naar streven en tegelijkertijd een belangrijke indicatie dat de beheerorganisatie stabiel en volwassener wordt.

3.3 Checks als input voor meting

De resultaten van checks kunnen worden gebruikt als input voor een nieuwe meting. Deze informatie en bewijslast zijn immers afkomstig uit eerste hand en zijn geborgd volgens het 4-ogenprincipe (uitvoerder versus reviewer).

Tips

- 1) Gebruik twee tabbladen in de webbrowser bij het afstemmen van de acts en checks met de meting. Open de meting in het eerste tabblad en het takenmanagement van het betreffende normenkader in het andere tabblad. Op deze manier kun je snel schakelen en kopiëren van het ene tabblad naar het andere. Door de URL van Key2Control te kopiëren naar een tweede tabblad in de webbrowser wordt de software opnieuw geopend.
- 2) Als een check van een norm meerdere keren is gepland in het lopende beheersjaar, dan is de laatste uitkomst de input voor de meting¹. Uiteraard beoordeel je ook andere resultaten om na te gaan of er sprake is van een normaal patroon en je betreft ook de input uit de vorige meting.
- 3) In gevallen waarin geen resultaten beschikbaar zijn uit een check, volg je dezelfde werkwijze als bij de eerste meting voor de betreffende norm. Uiteraard kun je daarbij gebruikmaken van de resultaten uit de vorige meting

Een groot voordeel is dat elke check dezelfde stuurvragen hanteert als de norm in een meting. De antwoorden op die stuurvragen kunnen eenvoudig worden overgenomen in de meting.

4 Objectenmodule

De objectenmodule heeft tot doel een verdiepingsslag te realiseren op het gebied van interne beheersing. Een object kan verschillende vormen aannemen en waarde hebben voor de organisatie, zoals een gebouw, computerruimte, ICT-infrastructuur, processen, informatiesystemen of patenten (intellectueel eigendom). Deze objecten dragen bij aan het bereiken van de bedrijfsdoelstellingen en kunnen via plannen worden gekoppeld aan normen uit verschillende normenkaders. Denk bijvoorbeeld in het licht van informatiebeveiliging aan het opnemen van alle kritische informatiesystemen in de objectenmodule en deze via plannen te koppelen aan relevante maatregelen in het normenkader informatiebeveiliging, of door het vastleggen van alle relevante subsidieregelingen en deze te koppelen aan relevante maatregelen in het normenkader subsidiebeheer. In paragraaf 4.1 wordt uitgelegd hoe je een object koppelt aan een taak.

De module kan ook worden gebruikt als centrale informatiebron voor objecten, zonder deze aan normen te koppelen of een combinatie daarvan. Denk bijvoorbeeld aan relevante documenten over een object die snel beschikbaar moeten zijn voor functies zoals concerncontroller, CISO, FG, jurist of privacyfunctionaris. Op die manier kan de module ook dienen als een digitaal documentdossier. In paragraaf 4.2 wordt uitgelegd hoe je de objectenmodule kunt gebruiken als digitaal documentdossier. In paragraaf 4.3

¹ Dit geldt niet voor checks die gekoppeld zijn aan een object. Immers elk object-gerelateerde check kan een andere uitkomst hebben. In dat geval worden alle objecten betrokken om een generieke uitkomst voor een meting te bepalen. Licht dit dan ook toe in het commentaarveld van de betreffende norm bij de meting.

wordt een voorbeeld uitgewerkt van het op een pragmatische wijze gebruik maken van de objectenmodule in het domein van informatiebeveiliging.

Tot slot is het belangrijk om op te merken dat de klant volledige vrijheid heeft in het gebruik van de objectenmodule. In de basis is de objectenmodule niet voorzien van content.

4.1 Objecten koppelen aan maatregelen

Objecten kunnen worden gekoppeld aan act- en checkmaatregelen waardoor een maatregel specifiek wordt voor het betreffende object. Zo kan bijvoorbeeld een kritisch informatiesysteem worden gekoppeld aan verschillende maatregelen die verband houden met logische toegangsbeveiliging. De reden hiervoor is dat je specifiek wilt weten of de logische toegangsbeveiliging adequaat geregeld is voor deze applicatie. Dit kan niet worden bereikt met een generieke aanpak. Zo is het mogelijk dat voor een checkmaatregel 20 taken zijn gepland, elk met een ander object waarvan het eindresultaat verschillend kan zijn.

Het koppelen van objecten aan een taak in het normenkader gebeurt onder de tab 'Opties' zoals hieronder weergegeven.

Check

9.2.6 Stel vast dat de toegangsrechten bij beëindiging zijn geblokkeerd

Algemeen Stuurvragen **Opties** Toelichting Taken

Object

Object

Aantal uren

Uurtarief

€

Kosten: -

Door met de cursor in het veld 'Object' te gaan staan en een linker muisklik te geven, verschijnen alle objecten in een pop-upvenster waar je doorheen kunt scrollen. Het is ook mogelijk om de naam van het object in te typen, zodat deze direct in het scherm verschijnt.

Tips:

- 1) Leg de nadruk bij het plannen vooral op die objecten waarvan bekend is dat ze extra aandacht nodig hebben op het gebied van interne beheersing. Dit geldt vooral voor die objecten die minder goed onder controle zijn. Hoe bepaal je dat? Op basis van eerdere resultaten en eigen waarnemingen.

- 2) Als er veel objecten zijn, denk dan na over een roulatieperiode waarbij in ieder geval alle objecten eens per 3 jaar gepland worden. Houd het pragmatisch en voorkom dat je honderden taken gaat uitzetten.
- 3) Stem de planning waarin objecten zijn opgenomen vooraf af met de betrokken uitvoerders (verwachtingsmanagement) vooral als dit de eerste keer is dat een uitvoerder hiermee te maken krijgt.
- 4) Beschrijf in de werkinstructie wat je van het betreffende object wilt weten en welke bewijslast eventueel opgeleverd moet worden.

Mijn taken

Onder 'Mijn taken' staan voor elke gebruiker de taken in de rol van uitvoerder en reviewer. Als een taak gekoppeld is aan een object, wordt dit weergegeven in het 'tegeltje' van de taak. Door de cursor op het object te plaatsen, verschijnt automatisch alle informatie, inclusief bijlagen, in een afzonderlijk scherm. De naam van het object is ook aan de rechterkant in het afhandelscherm zichtbaar en werkt op dezelfde manier als in het 'tegeltje'. De bijlagen kunnen gedownload worden, maar het is niet mogelijk om bestanden te uploaden. Uiteraard kunnen bestanden wel geüpload worden voor de betreffende taak zoals bewijslast waar het ook voor bedoeld is. Ter illustratie van deze functionaliteit is een printscreen opgenomen voor het object 'Suwinet'.

Suwinet	
Categorie	Informatiesysteem
Eigenaar	Gerrit Goud
Omschrijving	Suwinet is een kritische cloudapplicatie en valt onder de jaarlijkse ENSIA-audit. Met Suwinet kunnen gebruikers gegevens over adressen, inkomen en vermogen benaderen van elke inwoner in Nederland. In het verleden is dit behoorlijk fout gegaan door gegevens te raadplegen van bekende Nederlanders zonder enige grondslag. Het is dus super belangrijk dat wij ons houden aan de gestelde eisen op het gebied van de bescherming van persoonsgegevens en informatiebeveiliging.
Bestanden	230522 Autorisatiematrix Suwinet.docx 230522 Autorisatieprocedure Suwinet.docx 230523 Beveiligingsplan Suwinet 2023.docx 230523 Procedure controle op logging Su... Voorbeeld rapport controle logging detailg...

Opmerking: In het takenmanagement onder het normenkader worden de geplande taken gerelateerd aan objecten vermeld. Er wordt echter geen informatie weergegeven wanneer de cursor over het object beweegt. De reporter kan immers direct toegang krijgen tot de objectenmodule vanuit zijn rol.

4.2 Objecten als centraal verzamelpunt

De objectenmodule kan ook gebruik worden voor het vastleggen van documentatie per object. Denk bijvoorbeeld aan het object 'dataclassificatie' waarbij alle relevante documentatie wordt opgenomen om te raadplegen en bij te houden. Dit kan ook gelden voor verwerkersovereenkomsten of contracten, of het bijhouden van beveiligingsincidenten en datalekken. Voor de Wet politiegegevens (Wpg) die onder

een toezichts- en auditregime valt, is het handig om voor elk jaar een afzonderlijk object aan te maken. Hieronder kunnen dan alle relevante documentatie worden opgenomen zoals het verslag van bevindingen van de functionaris voor gegevensbescherming (FG), het interne auditrapport, beleidsstukken, procedures en richtlijnen die relevant zijn voor de toezichthouder, interne en externe auditor. Op deze manier kan de objectenmodule wordt gebruikt om de historie voor elk jaar bij te houden zoals geïllustreerd in het volgende voorbeeld.

Naam	Categorie	Eigenaar	
Wpg leerplicht / 2022	Wet politiegegevens	Gerrit Goud	Bekijken
Wpg leerplicht / 2023	Wet politiegegevens	Gerrit Goud	Bekijken
Wpg openbare ruimte / 2022	Wet politiegegevens	Gerrit Goud	Bekijken
Wpg openbare ruimte / 2023	Wet politiegegevens	Gerrit Goud	Bekijken

Een ander voordeel is dat er vanuit een meting direct verwezen kan worden naar de documentatie die onder het betreffende object is opgenomen. Dit geldt ook bij het uitvoeren van taken die gerelateerd zijn aan een object. Hierdoor is alle relevante informatie gemakkelijk toegankelijk en kan er efficiënter gewerkt worden.

Tips:

- 1) Open als reporter de objectenmodule in een apart tabblad, zodat deze altijd beschikbaar is om te raadplegen of te onderhouden
- 2) Denk na over het gebruik van categorieën om wildgroei te voorkomen. In het begin kan dit uit de hand lopen, maar dat is geen probleem, objecten kunnen altijd opnieuw worden gegroepeerd.

4.3 Praktijkvoorbeeld gebruik objecten / informatiebeveiliging

Als het gaat om het opzetten van een ISMS in Key2Control dan is een algehele aanpak om eerst te beginnen met generieke taken en daaraan geleidelijk specifieke taken (objectgerichte taken) toe te voegen. Dit maakt deel uit van een groeiproses. Door te beginnen met meten en het uitzetten van generieke taken, raakt de organisatie vertrouwd met de standaard beheersingsprincipes. Op basis van een risicoafweging worden keuzes gemaakt welke normen voldoende worden afgedekt door middel van 'meten' en welke normen regelmatig moeten worden gepland voor checks. De toegevoegde waarde van een risicoafweging ligt vooral in het voorkomen van onnodige werkdruk en het vinden van een juiste balans. Als uitvoerders overladen worden met

taken waarbij ze het gevoel hebben dat deze geen toegevoegde waarde hebben, dan zullen ze afhaken. Kortom, niet alle checks hoeven gepland te worden. Denk bijvoorbeeld aan informatiebeveiligingsbeleid waarbij tijdens de meting is vastgesteld dat aan alle eisen is voldaan. Het heeft dan weinig zin om hiervoor een check te plannen, wetende dat een update pas over 3 jaar nodig is.

Aan de andere kant groeit de behoefte om bepaalde normen te koppelen aan objecten. Op het gebied van informatiebeveiliging kun je bijvoorbeeld denken aan de logische toegangsbeveiliging of het documenteren van beheertaken van functioneel applicatiebeheerders. Als CISO wil je weten hoe dit geregeld is voor elk kritisch informatiesysteem. Dit kan niet worden vastgesteld met een generieke checktaak, maar vereist objectgerichte checktaken. Op deze manier betrekken we ook de functioneel applicatiebeheerders bij het intern beheersingsproces rond informatiebeveiliging, met als doel hun professionalisering verder te bevorderen. En dat is in het huidige digitale dreigingsbeeld een essentiële voorwaarde.

Van elk kritisch informatiesysteem is een object aangemaakt dat verrijkt kan worden met aanvullende informatie zoals aangegeven in paragraaf 4.2. Hierbij kan gedacht worden aan de resultaten van een dataclassificatie, inzicht in het gebruik van de applicatie, een autorisatiematrix, functionaliteiten van de applicatie, inzicht in persoonsgegevens, DPIA-uitslagen, eigen aantekeningen, enzovoort.

De CISO heeft de mogelijkheid om een object aan te maken voor het vastleggen van de resultaten van een dataclassificatie, of een object waarin alle relevante beleidsstukken, procedures en richtlijnen op het gebied van informatiebeveiliging zijn opgenomen voor intern gebruik. Op deze manier kan de CISO deze informatie eenvoudig beheren en indien nodig (laten) aanpassen, en toegankelijk maken voor toezichthouders en auditors. Bovendien is hiermee het kennisbehoud geborgd als sprake is van opvolgers. Het doel van deze vastlegging is niet om de boodschap uit deze documentatie te verspreiden. Daarvoor gelden de gebruikelijke communicatiekanalen van de organisatie naar medewerkers zoals het intranet. Dit betekent dat deze documenten gepubliceerd moeten worden als ze formeel zijn vastgesteld.

Tip

- 1) Als gebruik wordt gemaakt van objecten bij informatiebeveiliging dan is het aan te raden om ook het object 'Generiek' aan te maken. Dit object omvat taken die organisatiebreed gelden. Het voordeel hiervan is dat je deze taken eenvoudig kunt filteren en bekijken via het objectenfilter in het takenmanagement. Dit betekent wel dat elke geplande taak een bijbehorend object moet hebben, hetzij generiek of specifiek.

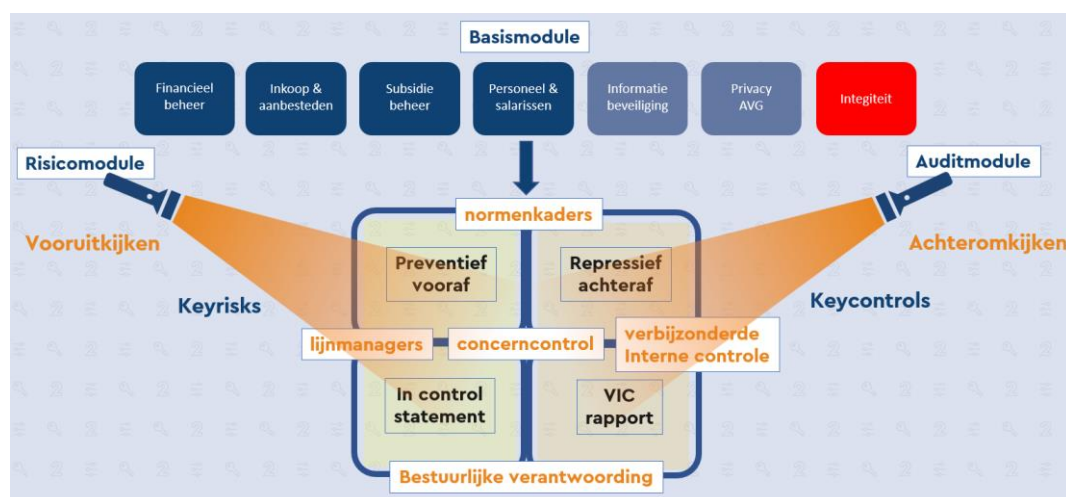
5 Beheersingsmodel en repeterende beheeractiviteiten

5.1 Algemeen

In dit hoofdstuk gaan we dieper in op relevante beheeractiviteiten die noodzakelijk zijn om het interne beheersingsproces levend te houden met ondersteuning van de software van Key2Control. De effectieve waarde van onze software is immers mede afhankelijk van de manier waarop de beheerorganisatie de regels van interne beheersing volgen. Daarom besteden we ook aandacht aan de relatie van onze software met het beheersingsmodel dat we als basis hanteren, evenals de gangbare interne beheersingsprincipes. Op die manier streven we ernaar om de software beter te begrijpen vanuit dit perspectief.

5.2 Intern beheersingsmodel in relatie tot Key2Control software

Onze software fungeert als een 'springplank' voor organisaties die nog worstelen met het ontwikkelen van een visie en beleid op het gebied van integrale interne beheersing en de implementatie ervan. Een van de grootste uitdagingen in dit vraagstuk is namelijk hoe de governance oftewel de organisatiebesturing rond interne beheersing vorm krijgt. Hierbij draait het vooral om de implementatie van het drielijnenmodel dat de governance ondersteunt door de rolverdeling en verantwoordelijkheden duidelijk te definiëren en de collectieve slagkracht te versterken. Op papier lijkt dit wellicht eenvoudig, maar in de praktijk blijkt dit een moeizaam proces te zijn. Enerzijds komt dit door een gebrek aan aansluiting van de 1^e lijn op het beheersingsproces en anderzijds doordat de 'poortwachters' in de 2^e lijn een eigen werkwijze hanteren die de onderlinge afstemming en samenwerking belemmert. En zo opereert iedereen vanuit zijn eigen 'bubbel'. Onze software ondersteunt die aansluiting en bevordert de onderlinge afstemming en samenwerking door gebruik te maken van voorgedefinieerde normenkaders vanuit een gestandaardiseerde aanpak die laagdrempelig is. Het beheersingsmodel in relatie tot onze software ziet er als volgt uit:



Centraal in het model staan de normenkaders die gepositioneerd zijn in onze basismodule. Controleren is namelijk het toetsen aan een norm. In dit voorbeeld zijn slechts een beperkt aantal normenkaders ter illustratie weergegeven. Elk normenkader bestaat uit een samengestelde set van toetsbare normen. Deze set normen is voorafgaand aan de samenstelling zorgvuldig bepaald door middel van een risicoanalyse, uitgebreid deskresearch en input en feedback van professionals.

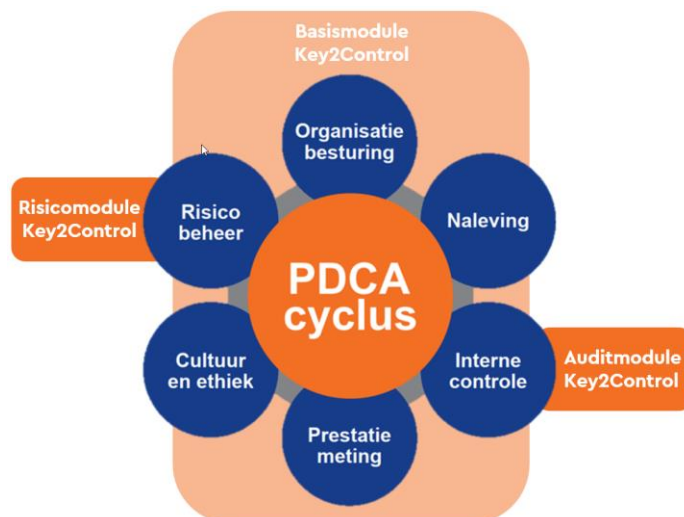
Door periodiek te meten wordt beoordeeld in hoeverre de normen geïmplementeerd (opzet en bestaan) zijn. Het verkregen beeld kan intern besproken worden met de betrokken verantwoordelijken waarbij gekeken wordt welke verbeteringen nodig zijn. Hierbij kan de 2e lijn advies geven. In de kern gaat het dus om periodieke zelfevaluaties met als doel verbeteringen door te voeren waar nodig en het bewustzijn rond interne beheersing in de 1e lijn te vergroten. Daarnaast kunnen deze resultaten gedeeld worden met andere belanghebbenden zonder de inhoud te hoeven kennen. Op grafische wijze is in 1 opslag al duidelijk wat de resultaten zijn van een zelfevaluatie en kan op basis van dat beeld een nader toelichting worden gegeven. Een gemiddelde score van 85% of 35% op twee verschillende metingen is al reden genoeg om de aandacht te richten op de meting met een lage score. Zo kan een concerncontroller op eenvoudige wijze een beeld vormen rond de resultaten van een meting op het gebied van informatiebeveiliging zonder de inhoud te kennen. Het delen van dit soort informatie creëert onderling vertrouwen. Voorts ontstaat met dit repeterend mechanisme een zelfreinigend vermogen in de organisatie waarmee de basis wordt gelegd voor een 'in control statement', die als grondslag dient (responsibility) voor het afleggen van bestuurlijke verantwoording (accountability).

Aan de linkerflank bevindt zich de risicomodule die het beheersingsmodel versterkt door de belangrijkste risico's (keyrisks) en bijbehorende beheersmaatregelen (keycontrols) in kaart te brengen. Met behulp van de risicomodule kan de organisatie sturen op de belangrijkste risico's, terwijl inzicht wordt behouden in andere normen die daar niet direct onder vallen, maar waar wel verantwoording over afgelegd moet worden. Door gebruik te maken van de risicomodule wordt als het ware gewichten aan de normen toegekend om zo de belangrijkste beheersmaatregelen te identificeren. Uiteraard biedt de risicomodule alle ruimte om ook risico's te beheren die geen relatie hebben met voorgedefinieerde normenkaders.

De rechterflank wordt versterkt door ondersteuning van de auditmodule waarbij ook gebruik kan worden gemaakt van de beschikbare normen uit de normenkaders. Hierdoor blijft de interne audit verbonden met zowel de 1e als de 2e lijn, wat de onderlinge samenhang en verbinding bevordert. Uiteraard biedt de auditmodule alle ruimte om ook buiten het pad van voorgedefinieerde normenkaders audits uit te voeren. Dit deel van de interne beheersing richt zich voornamelijk op het toetsen van de werking van de beheersmaatregelen.

5.3 Gangbare beheersingsprincipes in relatie tot Key2Control software

Als we onze software relateren aan de gangbare beheersingsprincipes van interne beheersing dan is de relatie als volgt:



Het hele spectrum van interne beheersing wordt ondersteund met onze software en is op twee onderdelen verbijzonderd in de vorm van een risicomodule en een auditmodule. Daarnaast ondersteunen wij ook de zachte kant van interne beheersing (cultuur en ethiek), ook wel bekend als de soft controls. Dit doen we enerzijds door middel van een apart normenkader voor integriteit en anderzijds door het gebruik van onze software als een middel om het collectieve bewustzijn en de slagkracht rond interne beheersing te verhogen.

Onze software heeft uiteraard input nodig om te verwerken en om output te kunnen genereren en te delen. Het leveren van input gebeurt echter niet vanzelf. Daarvoor zijn de beheeractiviteiten rond de PDCA-cyclus nodig, waarvan een deel behandeld is in hoofdstukken 2 en 3. Door dit zogenaamde 'vliegwiel' in beweging te brengen en vast te houden, ontstaat er een proces dat als het ware een aanzuigende werking heeft op de borging van de inhoud. Dit proces is - hoe vreemd het ook klinkt - belangrijker voor de continuïteit dan de inhoud zelf. Er zullen namelijk altijd 'kleine brandhaarden' (inhoudelijke kwesties) zijn die moeten worden aangepakt. Het gaat erom dat de organisatie deze brandhaarden tijdig ontdekt en er verantwoordelijk op reageert om escalatie te voorkomen. Uiteindelijk draait het om het vinden van een balans tussen het beheersingsproces en de inhoud, en dit is mede afhankelijk van de context, omstandigheden en ontwikkelingen waarin een organisatie zich bevindt.

5.4 Periodieke rapportages

Van belang is dat de reporter bij zijn planning rekening houdt met het periodiek opstellen van managementrapportages volgens de PDCA-cyclus. Dit vereist discipline en is ook heel herkenbaar als het gaat om de jaarlijkse rapportagecyclus van begroting, financiële voortgangsrapportage en jaarrekening. Het doel hiervan is om direct betrokkenen op een aantoonbare en formele manier mandaat te geven (voor verbeteringen), tussentijds op de hoogte te houden van de stand van zaken en jaarlijks verantwoording af te leggen. Daarnaast zijn deze documenten relevant om aan te tonen dat het interne beheersingsproces geborgd is. In essentie gaat het jaarlijks om de volgende rapporten:

Nr.	Document	opleveren
1.	Jaarplan jaar t	In januari / februari lopend jaar
2.	Voortgangsrapport jaar t	Na de zomer
3.	Verantwoordingsrapport jaar t	In januari / februari nieuwe jaar

Interessant is dat het opleveren van zowel het jaarplan als het verantwoordingsrapport in dezelfde periode valt, zij het dat het jaarplan toekomstgericht is en de verantwoording een terugblik vormt op het afgelopen jaar. In het kort behandelen we deze 3 rapporten afzonderlijk.

Tips:

- 1) Maak zoveel mogelijk gebruik van eigen rapportagesjablonen met een standaardindeling en opmaak. Houd de inhoud kort en kernachtig zonder teveel details.
- 2) Stem de behoefte van de directie en het bestuur hierop af om te voorkomen dat er onnodig veel tijd wordt besteed aan het opstellen van rapporten.
- 3) Zorg ervoor dat het opstellen van een rapport weinig tijd vergt door gebruik te maken van de rapportages en exports uit de software van Key2Control.
- 4) Rapporteer ook als er niets of weinig te melden is. Houd altijd de cyclus van rapporteren vast.
- 5) Upload de aangeboden rapportages aan de directie bij de norm van de openstaande meting waarop ze betrekking hebben, als bewijslast of neem ze op onder een daarvoor ingericht object.
- 6) Als er gebruik wordt gemaakt van meerdere normenkaders in de software, bijvoorbeeld in het kader van de financiële rechtmatigheid, is het aan te bevelen om al deze thema's op te nemen in één jaarplan, voortgangsrapport en verantwoordingsrapport, volgens eenzelfde opbouw. Net zoals je dat ook doet met een programmabegroting.

Opmerking: In alle rapportages in Word en pdf is het veld 'Omschrijving' toegevoegd aan het voorblad. Dit veld kan worden bewerkt voor elk meetnummer onder het tabblad 'Meten'. Raadpleeg hiervoor paragraaf 2.1.

Jaarplan

Elk nieuw beheersjaar begint met een meting als tijdstempel. Dat is een taak van de reporter en vergt na een eerste meting weinig tijd zoals aangegeven in paragraaf 2.1. Een belangrijk voordeel van een jaarlijkse meting is het creëren van een tijdlijn van de resultaten van het betreffende normenkader waardoor het mogelijk is een verschillenanalyse ten opzichte van de vorige meting uit te voeren. De percentages per hoofdstuk kunnen vanuit de software gekopieerd worden naar Excel in een tabel voor grafische verschillenanalyses. Als er twijfel is over de gegevens in Excel dan kan er altijd teruggevallen worden op de vaste gegevens in Key2Control. Deze vorm van terugkijken legt tevens een basis voor vooruitkijken, omdat het een verwachtingspatroon (trend) aangeeft in de vorm van een stijgende, dalende of gelijkblijvende tijdlijn.

Voor elke nieuwe PDCA-cyclus is de meting de eerste stap en tevens de basis voor een jaarplan. Het jaarplan geeft antwoord op de vraag waar we staan op basis van de meting en wat we het komende beheersjaar gaan verbeteren. Het jaarplan behoort formeel te worden vastgesteld door de directie waardoor de reporter het mandaat krijgt om de voorgenomen verbeteringen door te voeren in de vorm van acts die een hoge prioriteit hebben gekregen in de software van Key2Control.

Interessant is dat de verwachte verbeteringen ook kunnen worden vertaald naar een prognose van de meetresultaten. Met andere woorden, hoe zouden we scoren als we de geplande verbeteringen dit jaar realiseren. Hoewel de berekening en presentatie hiervan buiten de software plaatsvinden, bijvoorbeeld in Excel, is de benodigde basisinformatie beschikbaar in onze software.

Dezelfde meting voor het jaarplan dient tevens als basis voor het afleggen van verantwoording over het afgelopen beheersjaar. Deze terugblik kan worden versterkt met het uitvoeren van een verschillenanalyse waarbij de laatste meting wordt vergeleken met de vorige meting waarop het jaarplan is gebaseerd. Op deze manier ontstaat een naadloze overgang tussen het afronden van de vorige periode en het starten van een nieuwe periode.

Voortgangsrapport

Het voortgangsrapport geeft een beknopte samenvatting van de stand van zaken met betrekking tot de geplande acts volgens het jaarplan aangevuld met eventuele nieuwe omstandigheden en ontwikkelingen die niet in beeld waren tijdens de laatste meting². Daarnaast biedt dit rapport inzicht in eventuele achterstanden in de planning. Een extra

² Het gaat hier om de zogenaamde niet-planmatige verbeteringen, zie paragraaf 2.3.

toegevoegde waarde is het opnemen van de tussenstand van de lopende meting³ indien deze wordt bijgehouden. Hiermee kan worden aangetoond in hoeverre de actuele tussenstand zich verhoudt tot de stand van de meting waarop het jaarplan is gebaseerd en eventueel tot de prognose. Opvallende verschillen kunnen nader worden toegelicht.

Verantwoordingsrapport

Het sluitstuk van elk beheersjaar is een verantwoordingsrapport voor de directie en het bestuur. Hierin wordt weergegeven wat er gepland was, wat er bereikt is en wat de huidige stand van zaken is. De basisgegevens voor dit rapport worden ontleend aan de software van Key2Control, vergelijkbaar met hoe een jaarrekening financieel herleidbaar is naar de boekhouding. Op deze manier wordt er consistentie behouden en kan er op elk gewenst moment worden teruggegrepen op de gegevens. Het jaarplan en voortgangsrapport van hetzelfde beheersjaar dienen als basis, evenals de meest recente meting voor het jaarplan van het nieuwe jaar.

Verklaring van toepasselijkheid (VVT)

De verklaring van toepasselijkheid geeft inzicht in de status van alle normen binnen een normenkader. Deze verklaring biedt informatie over de samenhangende set van normen die getoetst kunnen worden, of een norm van toepassing is, en zo ja, of de norm volledig, gedeeltelijk of niet geïmplementeerd is. Daarnaast geeft de verklaring van toepasselijkheid een prioriteit aan voor normen die gedeeltelijk of niet geïmplementeerd zijn. Een verklaring van toepasselijkheid vormt de basis voor het opstellen van een 'in control statement' en kan als bijlage worden toegevoegd aan een jaarplan en/of verantwoordingsrapport. Indien er vragen ontstaan naar aanleiding van het verstrekken van een verklaring van toepasselijkheid, kan altijd worden teruggevallen op de meetgegevens en onderbouwing zoals opgenomen in de software van Key2Control.

5.5 Opstellen planningsschema

Uiteraard heeft een reporter naast het beheer van zijn normenkader(s) ook andere taken en verantwoordelijkheden. Om te voorkomen dat het eerder besproken 'vliegwiel' zoals beschreven in paragraaf 5.3 tot stilstand komt, is het handig voor een reporter om jaarlijks een eigen planningsschema op te stellen en zichtbaar te maken in zijn werkruimte, bijvoorbeeld op een prikbord of iets dergelijks. Een planningsschema is zeer praktisch en een uiterst effectief hulpmiddel.

Belangrijke beheeractiviteiten binnen de PDCA-cyclus die een reporter in zijn planningsschema kan opnemen zijn:

- a) Uitvoeren meting
- b) Bespreken resultaten meting

³ Zie tip 2 bij paragraaf 2.1

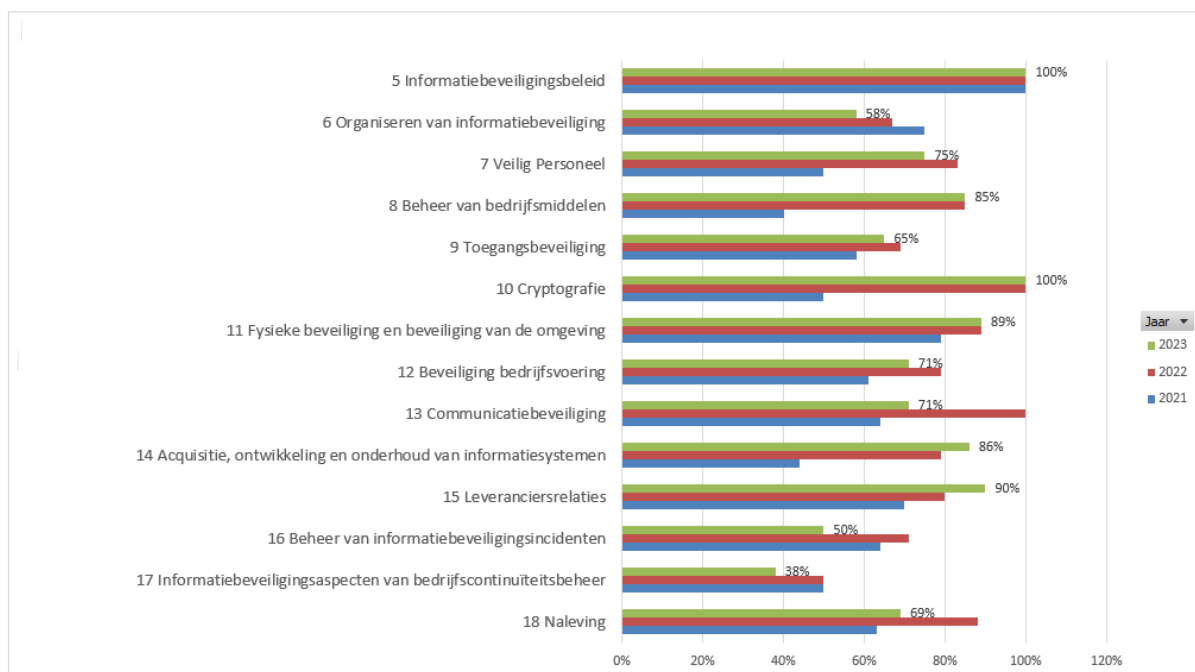
- c) Opstellen jaarplan
- d) Aanbieden jaarplan aan directie
- e) Prioriteren acts
- f) Plannen acts
- g) Afstemmen acts met uitvoerders
- h) Plannen checks
- i) Afsluiten vorig beheersjaar
- j) Opstellen voortgangsrapport
- k) Voorbespreking voortgangsrapport
- l) Aanbieden voortgangsrapport aan directie
- m) Uitvoeren nieuwe meting voor het nieuwe jaar
- n) Opstellen verantwoordingsrapport
- o) Voorbespreking verantwoordingsrapport
- p) Aanbieden verantwoordingsrapport aan directie

Uiteraard is het aan de reporter hoe hij hiermee omgaat en in welke volgorde en periode. Om het planningsschema nog strakker te maken kan het worden aangevuld met een tijdsindicatie zodat duidelijker wordt hoeveel tijd een reporter nodig heeft om het eerder genoemde 'vliegwiel' in beweging te houden. Op deze manier kan er gestuurd worden op een efficiëntieslag (tijdsbesparing) door gewend te raken aan het ritme van de PDCA-cyclus.

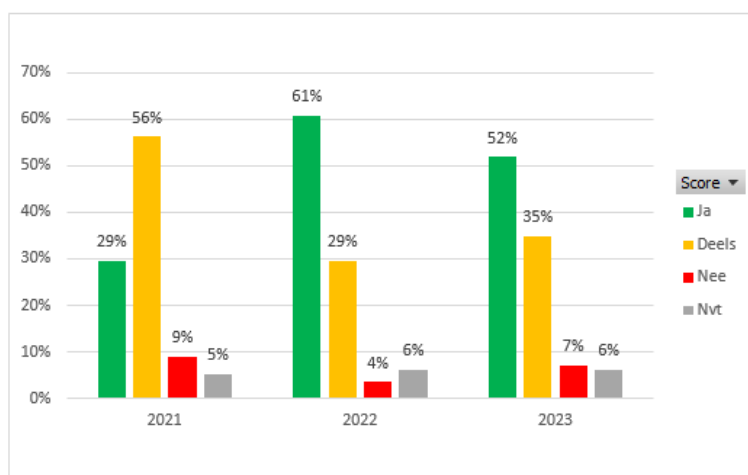
Het afsluiten van een beheersjaar (punt i) is belangrijk om te voorkomen dat taken per abuis gepland worden in oude beheersjaren. Je kunt dit vergelijken met het afsluiten van de boekhouding van het afgewikkelde jaar.

5.6 Beschikbare rapportages in Key2Control

Onze software bevat diverse rapporten en exports die kunnen worden gebruikt voor controle-, stuur- en verantwoordingsdoeleinden. Elke meting bevat drie rapporten die ook beschikbaar zijn als de meting nog niet is afgerond. Deze rapporten zijn zeer nuttig bij het tussentijds afstemmen van de resultaten van een meting. Een Verklaring van Toepasselijkheid legt de basis voor een 'in control statement' wat met name interessant is op het gebied van financiële rechtmatigheid. Het Excelbestand onder de meting is handig om te controleren of alle commentaarvelden bij de normen correct zijn ingevuld. Daarnaast kunnen er printscreens gemaakt worden van de grafische overzichten van de meting en kunnen de gemiddelde scores van een meting eenvoudig worden gekopieerd naar een Excelbestand voor het uitvoeren van een verschillenanalyse. Een voorbeeld hiervan kan er als volgt uitzien:



Het gaat hier overigens om een voorbeeld van een BIO-normenkader waarin de resultaten van 3-jaarlijkse metingen zijn opgenomen waarbij de gemiddelde percentages per hoofdstuk van het laatste jaar zichtbaar zijn gemaakt. Een ander voorbeeld is het weergegeven van de antwoorden van elke norm in een meting over de laatste 3 jaar, waarbij de groene staaf zo hoog mogelijk moet zijn.



Deze 3 rapporten zijn ook beschikbaar voor elk normenkader onder de knop "Rapportages" links van het scherm in Key2Control. Een belangrijk verschil is dat deze rapporten onder Meten eveneens beschikbaar zijn voor metingen die nog niet zijn afgerond. Daarnaast zijn er onder de knop "Rapportages" nog drie andere rapporten beschikbaar, waaronder een:

- Jaarplan (Word)

- Voortgangsrapportage (Word)
- Voortgang taken (Excel)

Jaarplan

Het jaarplan is beschikbaar zodra de meting is afgerond en bevat een inhoudsopgave die eenvoudig in Word kan worden voorzien van een verwijzing naar de betreffende pagina's (linkermuisklik → velden bewerken).

Tips:

- 1) Zorg ervoor dat alles in Key2Control is geprioriteerd als hoog of laag voor de betreffende meting. Als dit niet is gebeurd, doe dit alsnog en maak een nieuwe export.
- 2) Zorg ervoor dat de commentaarvelden bij de betreffende meting zijn ingevuld. Deze tekst wordt automatisch weergegeven bij de acts die als hoog geprioriteerd zijn gemarkeerd en nog niet zijn gepland. Als een act is gepland, dan wordt de werkinstructie bij de betreffende act vermeld in het jaarplan.

Met het jaarplan heb je een basis voor rapportage. Natuurlijk mag je hiervan afwijken en gebruikmaken van je eigen sjabloon. Je kunt de gegevens voor een jaarplan eenvoudig downloaden of kopiëren met behulp van exports uit de software.

Voortgangsrapportage

De voortgangsrapportage dient als basis voor het eigen voortgangsrapport. De reporter is uiteraard vrij om een eigen sjabloon te gebruiken. Een handige toevoeging voor gedetailleerde informatie is het Excelbestand "Voortgang taken". Hierin worden alle geplande taken (acts en checks) van het geselecteerde normenkader in het geselecteerde beheersjaar weergegeven, inclusief informatie zoals de status en meer.

6 Tot slot

Het doel van dit document is om onze klanten handvatten te bieden om meer rendement te halen uit onze software. Het document bevat talrijke tips die de stappen van meten, prioriteren, plannen en monitoren volgen. Daarnaast biedt het inzicht in de relatie tussen onze software en het beheersingsmodel dat wij hanteren, evenals de gangbare beheersingsprincipes, waaronder het gebruik van een PDCA-cyclus. Tevens is er aandacht besteed aan relevante beheeractiviteiten voor de reporters om het zogenaamde 'vliegwiel' rond de PDCA-cyclus voor hun normenkaders draaiende te houden.

Het gebruik van onze software draagt bij aan een grotere adoptie onder gebruikers en het realiseren van een stabiele beheerorganisatie door met name de ondersteuning van de 1e en 2e lijn bij hun beheeractiviteiten. Daarnaast biedt onze software functionaliteit

om het management actief te betrekken bij het interne beheersingsproces, zoals het verstrekken van stuur- en verantwoordingsinformatie..

Uiteraard is dit document dynamisch van aard. Er wordt immers voortdurend gewerkt aan de doorontwikkeling van onze software. Dit betekent dat er versiebeheer van dit document vereist is waar wij uiteraard aan voldoen.

Eventuele suggesties, feedback en tips van uw kant worden gewaardeerd, aangezien we graag samenwerken met onze klanten om het rendement van de software verder te vergroten.

U kunt daarvoor contact opnemen met klantondersteuning@key2control.nl

Einde document